Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 181 (2021) 477–486

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2020

Validation of Architectural Requirements for Tackling Cloud Computing Barriers: Cloud Provider Perspective

Bader Alghamdi[a,*], Leigh Ellen Potter[b], Steve Drew[c]

[a]*Faculty of Computer Science and Information technology, Albaha University, Albaha City 61008, Saudi Arabia*
[b]*IDEA Lab, Griffith University, Brisbane City 4111 , Australia*
[c]*Tasmanian Institute of Learning and Teaching University of Tasmania, Hobart 7005, Australia.*

Abstract

Although researchers and organisations have recognised cloud computing obstacles in the prior cloud adoption stage, few efforts have been made to investigate and address cloud barriers in depth during cloud implementation projects. The current technical cloud barriers faced by governments, such as a lack of cloud service availability and flexibility, a lack of application of service-level agreements (SLAs), and deficiencies in data security and privacy, require a proper strategic solution to elevate the role of enterprise architecture. This research designed and measured architectural requirements to overcome common technical cloud barriers. The architectural requirements were guided through The Open Group Architecture Framework (TOGAF) Architecture Development Method (ADM). The research employed a qualitative approach through three case studies to address the role of cloud providers. The findings of this research provide validation and overall support of the proposed value propositions with 12 identification-confirmed, newly emerged and designed architectural requirements, each of which can successfully contribute to overcoming barriers to government cloud projects. The elicited architectural requirements presented in the matrix are focused on the most important cloud constructs with different levels of emphasis.

Keywords: Cloud Computing; Enterprise information system; Requirements; TOGAF ADM.

* Corresponding author.
E-mail address: Baalghamdi@bu.edu.sa

10.1016/j.procs.2021.01.193

1. Introduction

Cloud computing use in public organisations has had significant positive impacts, including cost savings, improved agility, enhanced efficiency, better resource integration, more business opportunities and the simplification of complex work processes. Shared cloud computing services have been deployed on three main service architectures: Infrastructure as a Service (IaaS), in which infrastructure capabilities are hosted and managed by a provider; Platform as a Service (PaaS), which consists of system programming languages and libraries, also controlled by a provider; and Software as a Service (SaaS), which includes capabilities such as application interfaces and software for specific businesses [1]. Public organisations sometimes face barriers that prevent the full utilisation of cloud computing functions, such as a lack of cloud service availability and the failure of data privacy and security. Also, the increase in government cloud complex specifications have posed challenges for decision makers and practitioners to process and support successful cloud solution implementation [2, 3]. Therefore, overcoming cloud barriers requires appropriate guidelines and practices. Furthermore, other key factors in this process are understanding, linking and deploying underlying architectural requirements in alignment with stakeholder roles, such as that of a cloud provider, to tackle cloud barriers in a practical manner, which has been considered in this research in answer to a demand posed by [4]. Thus, the aim of this research, which is part of a larger research project, is to generate and evaluate architectural requirements to overcome dominant technical cloud barriers while also considering the roles of cloud providers using The Open Group Architecture Framework (TOGAF) Architecture Development Method (ADM). The following research questions directed this study: **RQ1,** what are the common technical cloud barriers to government cloud computing projects? **RQ2,** how can the identified enterprise architecture (EA) activities and cloud providers contribute to effectively tackling the recognised cloud computing barriers? The potential contributions are (1) to yield a validated matrix of architectural requirements in the body of an enterprise Information system (IS) and, potentially, in cloud governance activities, and (2) to use the developed requirements to improve the results of current government cloud computing projects by complementing TOGAF ADM activities with an empirical approach.

The remainder of this paper is structured as follows. Section 2 reviews literature related to common technical cloud barriers. Section 3 describes the research framework, whereby the design and management of architectural requirements are subject to TOGAF ADM activities. Section 4 demonstrates the research methodology, brief descriptions of the selected case studies, data collection process and case study analysis. Section 5 presents the findings, and Section 6 discusses these findings with a focus on the evaluation and implementation of the developed requirements. Section 7 illustrates the novel architectural requirements matrix (requirements validation and management). Finally, Section 8 concludes the research and proposes future work directions.

2. Literature Review

The most common cloud computing barriers, which were used as key constructs in the present study, are reviewed below. Each cloud concept is considered with respect to its potential application in government cloud computing.

Cloud service flexibility and availability are significant barriers due to a range of unpredictable events, such as connectivity failures at a provider's data centre, network infrastructure issues, and even road construction, which might affect network cables [5]. Clients expect to have optimal access to cloud services at any time via the Internet and have noted that availability is critical in public sectors, such as healthcare [6, 7]. Lee, Chae and Cho [8] identified such concerns around cloud adoption in a questionnaire-based study focused on the provider side in Korea. They found a major concern over cloud providers that could not always ensure service availability due to some technical failures [9]. Similarly, in the context of the government cloud in Saudi Arabia, Alsanea [10] identified insufficient IT infrastructure readiness as one of the major factors that hinders cloud service availability. Other scholars have claimed that cloud performance issues might occur when an application is unavailable due to low-speed connectivity or a system failure on the provider's side, which would violate Service Level Agreements (SLAs) [11-13]. However, a clear negative impact on enterprise businesses can be seen due to a lack of cloud service availability and flexibility, such as low service quality, low-speed connectivity and perhaps system failure on the provider's side. Thus, in order to address cloud service availability, the following value proposition is proposed: reducing the complexity and

customisation of cloud services and increasing the Quality of cloud Service (QoS) features can improve cloud service functionality and sustain mobile services.

Another technical cloud barrier is the application of SLAs and contracts between cloud providers and customers, which should be clarified by organisations prior to cloud migration (e.g. [12, 14, 15]). In research exploring three case studies of government and non-government organisations in Norway, El-Gazzar, Hustad and Olsen [6] described SLAs as one of the top 18 challenges in cloud adoption. In their study, SLAs were clearly identified as a cloud provider's responsibility. Lee, Chae and Cho [8], who studied enablers and inhibiters in the use of SaaS in Korea from a market and consumer perspective, identified the lack of suitable SLA standards as an economic factor inhibiting cloud adoption. They attributed the problem to cloud consumer beliefs and a business gap between suppliers and customers. El-Gazzar, Hustad and Olsen [6] and [8] failed to specify requirements for developing clear SLAs between cloud consumers and providers in the government context. Thus, in order to advance understanding of how to meet contract conditions within SLA application, clear architectural requirements are needed. Value Proposition: developing comprehensive SLA criteria, approving mandatory SLA requirements in alliance with cloud consumers, and identifying cloud provider responsibilities will meet contract conditions and obligations and sustain crucial cloud services activities.

Cloud data security and privacy within government cloud implementation are primary barriers, since government regulations prevent the storing of important data outside of government organisations or nations in general [6]. An evaluation study by Zwattendorfer, Stranacher, Tauber and Reichstädter [16] analysed government cloud adoption across eight European countries – Austria, Denmark, Finland, France, Germany, Ireland, Spain and the UK – and demonstrated that the most important barriers are data security and privacy. Other researchers have also identified these barriers as an ongoing and serious challenge in other developed countries, such as Australia and the US. Decision makers in government organisations are concerned about data security and privacy, and they are sceptical about cloud providers' abilities to deal with loopholes, network security, data accessibility and data confidentiality [16-19]. Kauffman, Ma and Yu [20] conducted exploratory research in which they claimed that security and privacy risks are the main barriers for both governments and non-governmental organisations in the context of Singapore. This view is supported by Paquette, Jaeger and Wilson [21], who described the intangible and tangible risks associated with the adoption of the federal government cloud in the US. They identified security and data access risks as a serious issue. Therefore, cloud data security and privacy required clear requirements to advance our understanding of cloud security attributes functionalities. Value proposition: developing solid security policy, utilising updated network security products and applying strict rules for data access, control and confidentiality will improve cloud data security and privacy.

Another critical factor is data sovereignty, which is defined as placing a data location 'in the border of a particular nation state, this is mainly for the purpose of verifying and controlling the geo-location of data in the cloud' [15]. Data sovereignty involves the geographical restriction of data storage and is a primary barrier to governments storing sensitive data. This issue has arisen during government cloud implementation in developed countries, such as the US and the UK [6, 7, 15, 22, 23], and poses concerns for decision makers due to differing government regulations and legal procedures for data privacy and governance [23, 24]. Irion [15] has argued that data sovereignty is a barrier for cloud providers, which control the physical storage of data, while El-Gazzar, Hustad and Olsen [6] demonstrated that, in Norway, geographical restrictions on data storage create obstacles for cloud providers. However, interpretations of this requirement vary depending on the type of cloud provider agreement, SLA and compliance requirements established by a cloud consumer organisation. Furthermore, a cloud provider's capabilities must be assessed to determine the SLA between the provider and risk management to mitigate, manage and identify tangible and intangible risks for government cloud implementation [15]. Value Proposition: hosting and locating physical data centres inside the country with strict access rules will increase the data sovereignty of the cloud project.

Interoperability and integration generally means the ability for different heterogeneous systems to function and interact together [25]; whereas in the cloud computing context, interoperability can be seen as the ability for multiple cloud platforms to run together. Issues with interoperability and integration in the cloud are due to a lack of consent standards, a lack of compatibility among services and inconsistencies among cloud provider platforms [22, 26, 27]. According to Chang, Walters and Wills [27], interoperability becomes a major barrier to cloud technology adoption due to differences among cloud platforms on the provider's side. Likewise, Zwattendorfer, Stranacher, Tauber and Reichstädter [16] identified interoperability and data portability, which are the responsibility of cloud providers, as

the main obstacles in the context of European government cloud adoption. This issue arises due to the rapid spread of cloud services in the market, with many different technical interfaces being offered to consumers by cloud providers. However, integration issues can hinder cloud implementation and can emerge when the current organisation's IT infrastructure has specific requirements or when there is a lack of standardisation between cloud providers and consumers [16, 28]. Irion [15] observed that integration is a vital concern for governments because moving from a legacy system to the cloud system requires full system utility. Khan, Ishaq, Khan and Soubani [18] examined cloud adoption by Saudi Arabian public higher education organisations to develop an educational cloud model, and among the barriers identified was interoperability between providers and consumers. Thus, the implementation of cloud projects in the government requires following proper standards to endorse interoperability and integration over all cloud platforms, systems and applications. Value Proposition: adopting open consent standards among cloud applications and detaching the legacy system will improve interoperability and integration.

3. Research Framework

The research problem assessed through TOGAF ADM was developed for the description and application of architectural requirements. This was done by careful review and comparison among the most common EA frameworks. Furthermore, given the complexity of cloud computing management imposed by contexts such as resources, business demands and stakeholders' engagement, having clear guidelines that support cloud providers is important for successfully engaging with and addressing the most dominant barriers to government cloud computing implementation [29]. Thus, the use of TOGAF ADM for high-level requirements in the present research would support the resolution of the identified cloud barriers through appropriate requirements, improving the IS strategic vision and business scenario for the government cloud context. This research employed ADM activities focused on the motivation and strategy phases in alignment with investigated cloud barriers. The required ADM phases are as follows: Preliminary Phase; Phase A, architectural vision; Phase H, architectural change management and requirements management. These phases, along with their artefacts, were used first to develop the necessary architectural requirements, and second to measure the suitability and applicability of these architectural requirements for overcoming cloud barriers as a robust strategic solution [30]. The researcher assumed that the current organisation had a good architectural model and defined the outcomes of the study relative to their EA [31]. Table 1 below presents the utilised ADM phases, artefacts, activities and outputs of each phase.

Table 1: Utilised ADM phases and artefacts (motivation and strategy).

TOGAF ADM Phases	Artefacts	Activities and Alignment of Cloud Constructs
Preliminary	Broad strategies, plan and assessment	Understand and evaluate the cloud barriers in terms of effect, frequency and domain existence.
	Organisational model and context	Define the government cloud computing context, projects, resources and capabilities.
Phase A: architectural vision	Governance and strategies	Define the solution vison and activities in relation to the cloud barriers.
	Roles of stakeholders	Select the key government cloud stakeholders.
	Cloud requirements, goals, principles and constraints	Identify and map requirements specifications, goals and architectural requirements.
Phase H: Architectural change management	Value realisation	Document and interpret all empirical evidence.
		Determine the final set of architectural requirements
	Management and monitoring	Combine the existing cloud system, process and standards with new designed requirements and reveal capabilities for future needs.
Requirements management	Requirements specification	Refine the list of simple, complete, consistent, correct and easy-to-understand requirements statements.
		Determine and change designed requirements based on qualitative findings.

Requirements impact assessment	Identify and manage potential ADM phases to be revised.
	Document and prioritise all designed architectural requirements in the architecture repository for cloud concepts (reference library).

4. Research Methodology

This research employed a qualitative approach through a case study methodology to gather rich information from related government cloud providers. The application of case study research, procedures and rules in the current study was guided through strategies that considered the case study questions, levels of analysis and standards for the interpretation of results [32, 33]. This research utilised three case studies in the context of Saudi Arabian cloud computing aimed at providing more robust research findings than could be obtained via the assessment of a single case study. The three cases have had experience designing, integrating and delivering government cloud computing-based services with robust IaaS, PaaS and SaaS solutions and EA capabilities. The three case studies compare several cloud products, such as government service bus (GSB), government secure network (GSN), E-portals, government resource planning, correspondence management, and cloud virtual server recovery (VSR). The three cases were coded as case A, case B and case C for anonymity. In light of Saudi Arabia's National Vision 2030, for which a number of national and local policies have been developed, the government is encouraging the use of emerging technologies, such as cloud computing, to reduce cost expenses and link and exchange smart services among government agencies [34]. Thus, the potential value can be realised in the selected context at a strategic level, at which organisations can determine current barriers in early project stages and govern their EA activities with appropriate requirements and practices.

The main source of information for this research were three sets of semi-structured interviews. The purposive sampling strategy was adopted to *recruit* the participants. Nine (9) participants comprising a mixture of both strategic-level (managers) and operational-level (practitioners) individuals from the three case studies (cloud providers) were identified. Using this sample of interview subjects ensured the accuracy and validity of the data from the shared cloud providers in Saudi Arabia. The interviews were conducted and recorded in a one-to-one manner in comfortable locations near to where the participants worked. Each interview lasted 45–60 minutes and was conducted in English. All interviews were transcribed, modified, analysed and coded using a hybrid approach (deductive and inductive analytical techniques) incorporating thematic analysis strategies. The deductive analysis technique enabled the placement of coded and categorised data into concepts in such a way that they corresponded with the proposed value propositions (designed architectural requirements). The inductive analysis technique complemented the deductive process and assisted the researcher in ensuring that no valuable concepts were missed, such as new concepts, requirements or sub-requirements. The triangulation of data sources was applied, thereby enhancing the robustness of the data *[35, 36]*. Lastly, the NVivo 11 software was used for data storage, ensuring that all findings were structured, revised and supported the capturing of potential meaning from real experiences.

5. Results

The results depicted the validation and overall support of the four main value propositions, which consisted of the designed architectural requirements with different levels of emphasis. The supported value propositions also resulted in 12 identification-confirmed and newly emerged designed requirements. The following quotes, written in *italics*, illustrate participants' views on the requirements. The data showed that cloud service flexibility and availability were not a barrier in the selected context – on the contrary, they were an enabler. All participants supported the proposition and belief that maintaining cloud service availability is a shared responsibility between cloud providers and consumers. For example, the participants indicated that *'including cloud service development in requests for proposals (RFPs) and SLA applications to meet client needs'* as well as *'forming a dedicated team to meet the operational service commitment'* would reduce the complexity and customisation of cloud services. Participants stated that *'engaging third parties in service development'* and '*having a dedicated operations team of both cloud providers and consumers to monitor the development process would support better cloud services'*. Regarding increasing QoS, the participants supported this statement by saying that focus should be placed on *'web application availability and*

precise response on service downtime, including service availability on SLAs'. The data revealed significant findings supporting cloud service delivery specifications: *'measuring and mentoring logs of transactions in both IaaS and SaaS layers per second to ensure real-time services'*, *'measurement of the pillars of cloud services'* and … *'tracking financial activities for cloud services'* would all contribute to annual organisational objectives as well as '*to monitoring high- and low-demand services'*. In terms of application of SLAs, the data revealed that the SLA was weak but was not a barrier. Developing comprehensive SLA criteria needs to be '*built based on clients' values, requests and needs, thereby leading to perfect QoS within the organisations*'. Although SLA designs emphasise '*designing the SLAs according to followed SDLC and service architecture standards, the customised matrices'* would support and sustain the performance of cloud services. SLA control was a challenge within the current '*organisational hierarchical structure*' in the Saudi context, one which hinders SLA performance. However, the SLA control requirements that emerged from the data indicated that '*revising and updating SLA activities periodically*' and ensuring that '*internal SLAs comply with external SLAs*' can enable SLA control. The Saudi IT regulations and authorities already '*enforce the use of SLAs in RFPs and contracts among cloud providers*'. Participants said that '*the proposal for SLA activities by cloud providers*' can '*help bridge the gap between clients and providers and govern the agreed mandatory requirements*'. Similarly, participants asserted that '*cloud providers should be included at the strategic level with cloud consumers and have legal and business teams'* to focus on the important matrices of SLAs, such as '*the number of transactions, response time, monitoring services, downtime and after sales*'. Cloud data security and privacy were found to not constitute barriers, although they do continue to present challenges. The data supported the value proposition and incorporated data sovereignty as a part of security activities. All participants stated that '*security requirements documented in RFPs and SLAs from the beginning,'* and '*adopting internal/external cloud security standards and privacy for clients*' were important, while security control required '*an established privacy security office/unit, and the application of data integrity practices to employees*'. The data showed operational security specifications, such as '*utilising security products to detect and prevent "working in prevention stage", performing regular assessments of security policies for vulnerable points, and periodically updating the cloud security software*', '*deploying GSN products among government agencies*', '*performing two-factor authentication and adopting network software for a public/private key matrix*' are important industrial practices. Most participants agreed on '*using data classification, granting the right access to the right stakeholder, ensuring data classification in compliance with cloud hosts* and having a '*prices data exchange model and international standard*'. Surprisingly, data disaster recovery (DDR) was a newly emergent requirement and the best fit for the data security category by '*establishing redundant backup data in a confidential location*, *initiating project data ownership'*. Lastly, in response to increasing data sovereignty, cloud data sovereignty is placed under cloud data security and privacy and can be achieved via '*the physical location of data needs to be hosted inside the country'*. Interoperability and integration were not considered to be barriers, as the participants '*stressed launch time, where major interoperability and integration issues appear and need to be documented*' to diagnose the issues; they then focused on '*technical-level PaaS, where multi-system and functional services are operated*'. Further analysis showed that the Saudi context '*deployed a cooperative solution among cloud providers*', one where '*internal and consistent standards, named YAFI, have been dedicated to tackling some cloud integration issues*'. YAFI is an Arabic term that means 'meet your needs', but it is used here to denote the integration architectural framework, which includes '*data and service portability inside the government cloud systems or with other stakeholders* [government agencies]'. Participants asserted that '*government cloud systems should be based on a single interoperability requirement, as well as being documented in cooperation with cloud consumers'*. In the meantime, participants stated that the use of a '*legacy system is a serious issue facing government cloud computing implementation on clients' sites but not on providers' sites*'. In order to address this challenge, the cloud providers requested the '*definition of legacy system functionalities*' through a product named '*GSB express, which has been built and installed at cloud consumers' sites to determine important functionalities as a technical adopter*'. Lastly, providers emphasised '*establishing a cloud migration plan and upgrading the technology equipment and software*'.

6. Discussion

The discussion and assessment outlined here were based on rates given by participants and reveal the degree to which the discussed cloud barriers have been or are being addressed. The results indicate that cloud service flexibility

and availability are not barriers; however, they *do* require a significant amount of effort to serve as enablers. Reducing complexity and customising cloud services ranked high among providers. The present findings appear to be consistent with those of other studies, which found that high levels of service customisation would negatively influence the flexibility of services and raise concerns over the deployment of cloud service performance [37, 38]. Thus, cloud services should be governed based on client needs, skilled teams and robust cloud IaaS. These findings are broadly consistent with those revealed in [6, 39]. Increasing QoS had strong support and ranked high with the emphasis on using service development models, such as Service Oriented Architecture (SOA) and SDLC, and precise response on service downtime in both PaaS and SaaS layers. These findings were previously discussed on a theoretical basis by [7, 40], and a possible explanation for this result is the alignment between EA guidelines and the goals associated with understanding the role of cloud providers. Confronting cloud service delivery specifications was ranked high by the providers and consisted of monitoring services within regular KPIs and tracking financial activities for each service. These practices were suggested on an abstract level in previous studies without specifying corresponding actions [23, 41], which may be due to the current context-driven stage of cloud computing use in Saudi Arabia. The SLAs application cloud construct represents challenges in this context because of the lack of SLA adoption on the consumer side. It is interesting to note that improved SLA implementation activities are clearly associated with QoS [42]. So, developing comprehensive SLA criteria ranked high, with providers adopting an SDLC model and engaging related departments to sustain the performance of cloud services. A possible explanation for this is that there is a clear understanding of a provider's duties towards Saudi cloud consumers. Also, the IT authority in this context enforces the use of SLAs among cloud providers as a compulsory factor in granting licenses to providers. This confirms Rimal, Jukan, Katsaros and Goeleven [23] assertion that says cloud service delivery as a contract with mature providers is an important architectural issue. Controlling SLA activities to comply with the SLAs of internal/external organisations is consistent with previous studies [6, 12]. However, there are complications in SLA control and negotiation because of hierarchical structures and low awareness among cloud consumers in the Saudi context. Clarifying SLA responsibilities in alliance with cloud consumers had a high ranking, and the data showed that providers help govern the agreed-upon mandatory SLA actions to meet corresponding commitments. This finding is consistent with those provided in other research [14, 21]. Clarifying the responsibility of cloud providers involved focusing on important matrices for consumers. This explains the relatively good alignment between the SLA practices of cloud providers and IT architecture practices. On the other hand, cloud data security and privacy presented ongoing challenges, and providers ranked high the development of a solid security policy, one which consists of strategies, policies and procedures, thereby ensuring security in RFPs and SLAs and prioritising actions on the basis of use cases. Only a few studies suggested these security actions as common practices [6, 10], but this research contributed by answers the 'how' questions through clear business and IT mechanisms and in terms of security. Utilising updated network security is already ubiquitously established in network access products in contexts such as the GSN. This finding is inconsistent with studies that discussed the network as an important factor in cloud adoption [24, 43]. Meanwhile, applying strict rules for data access, control and confidentiality ranked high. Although previous research, such as [20], offered some solutions related to data access barriers, the present study found that in-depth practices with the encountered stakeholders must be deployed in a continuous manner to support data assurance upon shared data resource pooling in compliance with regulations. This is a significant finding, one which shows that IT capabilities are being driven by regulations. Establishing a DDR site to store redundant backup data at a confidential location ranked medium. This is a fundamental requirement that emerged from the data and corroborates findings in previous studies [6, 7]. Lastly, data sovereignty (as part of the security practices) was ranked as low impact. The case study analysis revealed that the providers already include hosting and locating physical data centres inside the country with strict access rules. This was supported by Mutavd [44], who suggested that the use of privately hosted government cloud centres is a suitable solution for controlling data sovereignty. The interoperability and integration constructs are not barriers due to the enhancement of cloud interoperability convergence and integration across platforms in the selected context. Adopting consent standards among cloud providers' platforms was ranked high. Previous studies included limited discussions of integration issues, such as compatibility and data migration, identifying them as important factors without providing details about how data should be tracked and fixed [3, 45]. This exploration revealed that providers cooperated on the integration and performance of YAFI products—all leading towards better PaaS multi-system integration; these findings are on par with those of previous studies, which requested better data portability through common standards [40]. From a technical perspective, Alghamdi, Potter and Drew [46] discussed SOA governance and indicated the use

of the YAFI standard in SOA projects, but not cloud-based projects, in the Saudi context; however, the results presented here demonstrated a mechanism of services in the cloud-based environment, whether they are heterogeneous or homogeneous. This can possibly be attributed to the current modern IaaS and PaaS layers used on the sites of cloud providers. Finally, detaching legacy systems was ranked medium, with a noticeable level of support, and revealed steps to gradually bridge the gap between cloud providers and consumers. In the selected context, the legacy system was linked with GSB express to start data portability and reduce possible integration issues. This unanticipated finding was remarkable and was not previously described; it also answered questions posed by Gill, Smith, Beydoun and Sugumaran [47], who suggested the establishment and use of practical requirements to tackle interoperability issues. These practices explained the relative EA capabilities and readiness of the cloud projects in the selected context.

7. Requirements validation and management

The findings showed that the designed requirements were effective and supported tackling the discussed barriers. The achieved value propositions discussed here demonstrated valuable insights into how cloud providers contribute to tackling cloud barriers with necessary requirements. The requirements impact assessment mentioned here requires that information from several resources, such as requirements specification, cloud providers, impacts on context and potential ADM phases, be revised for the second ADM lifecycle. This technique was partly inspired by TOGAF ADM guidelines, section 27.4, The Open Group [31] and Utomo [48]. Table 2 presents the novel architectural requirements, their impact on the selected context, the TOGAF ADM phases to be revised, as well as the achieved value propositions.

Table 2: Novel architectural requirements matrix.

Constructs		Architectural Requirements	Impact / Priority	TOGAF ADM phases to be revised	Value propositions
Cloud service flexibility and availability	**R1**	Reduce complexity and customization of cloud services	High	Preliminary, Phase B, Phase C, Phase D, Phase E, Phase F, Phase G and Phase H.	Improve cloud service functionality.
	R2	Increase Quality of cloud service (QoS)	High		Facilitate sustainable mobile services.
	R3	Confront cloud services delivery specifications	High		
SLAs application	**R4**	Develop comprehensive SLA criteria	High	Phase D, Phase G and Phase H.	Meet contract conditions and obligations.
	R5	Clarify and approve mandatory SLA requirements and responsibilities in alliance with cloud consumers	Medium		Sustain crucial cloud activities.
Cloud data security and privacy	**R6**	Develop solid security policy	High	Preliminary, Phase B, Phase C and Phase D.	Enhance data accessibility and control.
	R7	Apply strict rules for data access, control and confidentiality	High		
	R8	Establish Data Disaster Recovery (DDR)	Medium		Introduce robust network security.
	R9	Utilize updated network security products	Low		
	R10	Hosting and locating physical data centers inside the country with strict access rules	Low		Achieve data residency and governance.
Interoperability and integration	**R11**	Adopt open and consent standards among cloud applications	High	Phase A, Phase B, Phase C, Phase D, Phase E and Phase F.	Deliver a unified integration cloud framework.
	R12	Detach legacy systems	Low		Reduce the risk of the legacy system.

Preliminary, Phase A= Architecture vision, Phase B= Business architecture, Phase C= Information system –(Data + Application architecture), Phase D= Technology architecture, Phase E= Opportunities and solution, Phase F= Migration planning, Phase G= Implementation governance, Phase H= Architecture change management.

8. Conclusion

This study set out to develop and evaluate architectural requirements to tackle common technical cloud barriers based on TOGAF ADM activities. The study reviewed the relevant literature covering technical cloud concepts. In light of the research questions mentioned in the introduction, the identification of technical cloud barriers was discussed and assessed to understand these barriers in detail. The study used a qualitative approach through multiple case studies to explore and understand the research issue in Saudi Arabia. The cloud providers showed great support for the value propositions, with a total of 12 novel architectural requirements with different levels of emphasis and impacts. The most significant point revealed here is that SLA applications, cloud data security and privacy continue to pose challenges as a consequence of some internal practices and external influences from cloud consumers' sites; as such, more effort is required to overcome them. On the contrary, cloud service availability and flexibility, as well as interoperability and integration, are not barriers. Designing and measuring the suitability and applicability of the architectural requirements via TOGAF ADM represent substantial contributions in the field of enterprise information systems. The current study has certain limitations, such as the selected TOGAF ADM, which consisted of many details and was therefore hard to utilise in all its capacities due to time limitations. The designed requirements are also not stable because of the time gap between their design and actual implementation. Future research will cover strategic cloud barriers, including the lack of organisational strategy, compliance, and culture and cost calculation issues, each of which should be investigated with proper requirements to facilitate a comprehensive cloud governance solution. The role of cloud consumers will be examined, and ArchiMate modelling will be used to present use case concepts.

9. References

[1] P. Mell, T. Grance.(2011) "The NIST definition of cloud computing [Recommendations of the National Institute of Standards and Technology-Special Publication 800-145]," *Publisher*, City.

[2] Y. Masuda, M. Viswanathan.(2019) "Enterprise Architecture for Global Companies in a Digital IT Era: Adaptive Integrated Digital Architecture Framework (AIDAF)," *Springer*, Singapore Pte Ltd.

[3] A. Mondorf, M.A. Wimmer.(2016) "Requirements for an Architecture Framework for Pan-European E-Government Services," in, *Springer International Publishing*, Cham, **pp. 135-150**.

[4] A. Cabrera, M. Abad, D. Jaramillo, J. Gómez, J.C. Verdum.(2016) "Definition and Implementation of the Enterprise Business Layer Through a Business Reference Model, Using the Architecture Development Method ADM-TOGAF," in, *Springer International Publishing*, Cham, **pp. 111-121**.

[5] B. Charif, A.I. Awad.(2014) "Business and Government Organizations' Adoption of Cloud Computing," in: Intelligent Data Engineering and Automated Learning–IDEAL 2014, *Springer*, **pp. 492-501**.

[6] R. El-Gazzar, E. Hustad, D.H. Olsen.(2016) "Understanding cloud computing adoption issues: A Delphi study approach," *Publisher*, City.

[7] S. Tweneboah-Koduah, B. Endicott-Popovsky, A. Tsetse.(2014) "BARRIERS TO GOVERNMENT CLOUD ADOPTION," *Publisher*, City.

[8] S.-G. Lee, S.H. Chae, K.M. Cho.(2013) "Drivers and inhibitors of SaaS adoption in Korea," *Publisher*, City.

[9] B. Alghamdi, L.E. Potter, S. Drew.(2017) "Desinge and implementation of government cloud computing requirements: TOGAF," in: IEEE 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), *IEEE*, Lombok, Indonesia, **pp. 1-6**.

[10] M. Alsanea.(2015) "Factors Affecting the Adoption of Cloud Computing in Saudi Arabia's Government Sector," in, Doctoral thesis, Goldsmiths, University of London.

[11] M.A. Hana.(2013) "E-government cloud computing proposed model: Egyptian E_Government Cloud Computing," in: Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on, **pp. 847-852**.

[12] E.Z. Milian, M.M. Spinola, R.F. Gonçalves, A.L. Fleury.(2014) "An Analysis of the Advantages, Challenges and Obstacles of Cloud Computing Adoption to an Academic Control System," in: Advances in Production Management Systems. Innovative and Knowledge-Based Production Management in a Global-Local World, *Springer*, **pp. 564-571**.

[13] V. Chang, R.J. Walters, G.B. Wills.(2015) "Cloud Computing and Frameworks for Organisational Cloud Adoption," *Publisher*, City.

[14] S. Haag, A. Eckhardt.(2014) "Organizational cloud service adoption: a scientometric and content-based literature analysis," *Publisher*, City.

[15] K. Irion.(2012) "Government cloud computing and national data sovereignty," *Publisher*, City.

[16] B. Zwattendorfer, K. Stranacher, A. Tauber, P. Reichstädter.(2013) "Cloud Computing in E-Government across Europe," in: Technology-Enabled Innovation for Democracy, Government and Governance, *Springer*, **pp. 181-195**.

[17] T. Oliveira, M. Thomas, M. Espadanal.(2014) "Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors," *Publisher*, City.

[18] F.Q. Khan, M. Ishaq, A.I. Khan, B. Soubani.(2014) "Adapting Cloud Computing in Higher Education," *Publisher*, City.

[19] R. Kurdi, A. Taleb-Bendiab, M. Randles, M. Taylor.(2011) "E-Government Information Systems and Cloud Computing (Readiness and

Analysis)," in: Developments in E-systems Engineering (DeSE), 2011, **pp. 404-409**.
[20] R. Kauffman, D. Ma, M. Yu.(2016) "A metrics suite of cloud computing adoption readiness," *Publisher*, City.
[21] S. Paquette, P.T. Jaeger, S.C. Wilson.(2010) "Identifying the security risks associated with governmental use of cloud computing," *Publisher*, City.
[22] M.A. Aziz, J. Abawajy, M. Chowdhury.(2013) "The Challenges of Cloud Technology Adoption in E-government," in: Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on, **pp. 470-474**.
[23] B.P. Rimal, A. Jukan, D. Katsaros, Y. Goeleven.(2011) "Architectural requirements for cloud computing systems: an enterprise cloud approach," *Publisher*, City.
[24] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica.(2010) "A view of cloud computing," *Publisher*, City.
[25] Z. Zhang, C. Wu, D.W. Cheung.(2013) "A survey on cloud interoperability: taxonomies, standards, and practice," *Publisher*, City.
[26] A. Mukhametzhanova, R. Harvey, D. Smith.(2014) "Ahead in the G-clouds: Policies, Deployment and Issues," in: Electronic Government and the Information Systems Perspective, *Springer*, **pp. 292-306**.
[27] V. Chang, R.J. Walters, G. Wills.(2014) "Review of Cloud Computing and existing Frameworks for Cloud adoption," *Publisher*, City.
[28] R.F. El-Gazzar.(2014) "An Overview of Cloud Computing Adoption Challenges in the Norwegian Context," in: Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on, *IEEE*, **pp. 412-418**.
[29] A.S. Zalazar, L. Ballejos, S. Rodriguez.(2017) "Analyzing Requirements Engineering for Cloud Computing," in: M. Ramachandran, Z. Mahmood (Eds.) Requirements Engineering for Service and Cloud Computing, *Springer International Publishing*, Cham, **pp. 45-64**.
[30] The Open Group.(2014) "The Open Group Cloud Ecosystem Reference Model," in: Requirement Managment, *The Open Group*, Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, United Kingdom, **pp. 88**.
[31] The Open Group.(2011) "The Open Group Standard TOGAF® Version 9.1," in, *The Open Group*, U.S. .
[32] R.K. Yin.(2014) "Case Study Research Design and Methods," 5 ed., *SAGE Publications, Inc*, USA.
[33] J.W. Creswell.(2013) "Qualitative inquiry and research design: Choosing among five approaches," *Sage*,
[34] Council of Economic and Development Affairs.(2016) "National Transformation Program 2020," in: P.M. Office (Ed.), *Media Center*, Saudi Arabia, **pp. 1-57 PP**.
[35] N.K. Denzin.(2017) "The research act: A theoretical introduction to sociological methods," *Routledge*,
[36] M.Q. Patton.(1999) "Enhancing the quality and credibility of qualitative analysis," *Publisher*, City.
[37] H. Nuseibeh.(2011) "Adoption of Cloud Computing in Organizations," in: In Proceedings of the 17th Americas Conference on Information Systems, Detroit, Michigan August 4-7th, **pp. 1-8**.
[38] S.M. Salleh, S.Y. Teoh, C. Chan.(2012) "Cloud Enterprise Systems: A Review Of Literature And Its Adoption," in: In PACIS, **pp. 76**.
[39] S. Schneider, A. Sunyaev.(2015) "CloudLive: a life cycle framework for cloud services," *Publisher*, City.
[40] V. Chang.(2015) "Delivery and Adoption of Cloud Computing Services in Contemporary Organizations,"
[41] M. Mreea, K. Munasinghe, D. Sharma.(2016) "A strategic decision value model for cloud computing in Saudi Arabia's public sector," in: 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), *IEEE*, **pp. 1-7**.
[42] A. Benlian, M. Koufaris, T. Hess.(2011) "Service quality in software-as-a-service: Developing the SaaS-Qual measure and examining its role in usage continuance," *Publisher*, City.
[43] H. Mouratidis, S. Islam, C. Kalloniatis, S. Gritzalis.(2013) "A framework to support selection of cloud providers based on security and privacy requirements," *Publisher*, City.
[44] R. Mutavd.(2010) "Cloud computing architectures for national, regional and local government," in: MIPRO, 2010 Proceedings of the 33rd International Convention, *IEEE*, **pp. 1322-1327**.
[45] F.F. Alruwaili, T.A. Gulliver.(2014) "ISPC: An Information Security, Privacy, and Compliance Readiness Model for Cloud Computing Services," *Publisher*, City.
[46] B. Alghamdi, L.E. Potter, S. Drew.(2016) "Identifying Best Practices in organisational SOA Governance Adoption: Case Study of Saudi Arabia's E-Government Programme," in: 20th Pacific Asia Conference on Information Systems,(PACIS 2016) Proceedings, Chiayi, Taiwan.
[47] A.Q. Gill, S. Smith, G. Beydoun, V. Sugumaran.(2014) "Agile enterprise architecture: a case of a cloud technology-enabled government enterprise transformation," in: PACIS 2014 Proceedings Paper 121.
[48] D. Utomo.(2014) "A Framework for Cloud Adoption from Enterprise Architecture and Business Perspective," in: School of Management and Governance, *University of Twente (UT)*, Enschede, The Netherlands.